Remarks/Arguments

Claims 1-7 are pending. No Claims have been amended as part of this response. Reconsideration of this application is respectfully requested.

Claims 1-7 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Chaney (United States Patent No. 6,035,037) in view of Shamir ("How To Share a Secret", Adi Shamir, MIT, Communications of the ACM, 1979, v. 22, no. 11). Applicant respectfully traverses these rejections, and submits all of the pending claims are patentably distinguishable over the cited prior art references for at least the reasons discussed below.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).* Further, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P. 706.02(j).* Further yet, the teaching or suggestion to make the claimed combination must be found in the prior art, and not based on the applicant's own disclosure. *In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).*

In the present case, the Examiner has failed to establish a *prima facie* case of obviousness, as the cited references, even when combined, fail to teach or suggest all the limitations of claim 1.

The present invention employs the concept of **secret sharing** which eliminates the requirement for using public key cryptography to ensure secure transmission of the audio/video stream from a service provider (page 5, lines 4-7). In one embodiment, a first seed value received in a smart card, and a second seed value, permanently stored in the smart card are used to generate a symmetric key (page 5, line 31 - page 6, line 20). In that regard, claim 1 recites *inter alia*:

(c) generating said scrambling key using said first seed value received in said smart card and a second seed value in a predetermined function, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card.

The combination of Chaney and Shamir fails to teach or suggest generating a scrambling key in a smart card using a first seed value received by the smart card and a second seed value permanently stored in the smart card, and thus fails to render Claim 1 unpatentable under 35 USC 103(a).

Specifically, Chaney teaches a system that uses first and second smart cards to produce an image that includes multiple image portions, such as picture in picture (PIP) or picture outside picture (POP). In this regard, the system of Chaney uses the known system of using entitlement management messages (EMM) and entitlement control messages (ECM), which are transmitted with the digital video stream, to control access to the video programs. According to Chaney, the key stored in the card is used to descramble the ECM to generate initialization data, which corresponds to the key received in the card. The initialization data is then used in another algorithm to generate the final descrambling key. Thus, the stored key is used to derive the received key, which in turn is used to derive the descrambling key with another algorithm.

In contrast, the method of Claim 1 uses both the stored key **and** the received key in a predetermined function, whereby secret sharing is implemented. Chaney says nothing about, and provides no teaching or suggestion, regarding secret sharing. Furthermore, the key stored in the smart card of Chaney is used for an entirely different purpose, and in a different manner, than that according to the method of Claim 1.

The Shamir reference fails to remedy the above-identified shortcomings of Chaney. Shamir, like Chaney, fails to teach or suggest using both a **permanently stored seed value** and a **received seed value** in a predetermined function to implement secret sharing. In fact, the Shamir reference expressly **teaches against** such a configuration. Instead, Shamir teaches that the mechanism that uses key shares (e.g., a key-share function implementing device) should **not** contain any secret information (i.e., the device does not store or contain the key shares). Furthermore, proper motivation does not exist for modifying the teachings of Chaney and/or Shamir to store a share or seed value in the smartcard.

Shamir explains its key sharing through the disclosed example of digitally signing checks. *See, col. 2.* Shamir teaches a standard solution that uses three executive signatures per check, and thus implements a (3, n) threshold scheme.

See, col. 2. Shamir further explains that each company executive would receive a key share D_i, and the company's signature generating device accepts any three of them to generate (and later destroy) a temporary copy of the company's actual signature key *D*. *See, col. 2, second full paragraph.* Shamir expressly teaches that "[t]he [signature generating] device does not contain any secret information and thus it need not be protected against inspection." *See, col. 2 (Emphasis added).* Accordingly, Shamir expressly teaches that devices that implement secret-sharing functions should **not** contain any secrets, such as key shares.

In contradistinction to the Shamir reference, Claim 1 clearly recites use of two seed values with one value being received in, and the other *permanently stored* by a smart card, to generate a scrambling key. As Shamir teaches against storing secret key shares in a signature generating device (such as the smart card of Claim 1), no combination of Shamir with Chaney would enable one of ordinary skill in the art to arrive at the invention as claimed in present Claim 1.

Accordingly, as neither Shamir nor Chaney teach or suggest "(c) generating said scrambling key using said first seed value received in said smart card and a second seed value in a predetermined function...said second seed value being permanently stored in said smart card;" their combination necessarily fails to teach these features and limitations.

Moreover, Shamir's disclosure of a method of secret sharing, wherein a key is divided into pieces and where the keys are combined in a device that expressly does not contain key shares, fails to provide any motivation for one skilled in the art to modify Chaney to somehow receive, in the smart card, data representative of a first seed value and further generate the scrambling key using the first seed value received in the smart card and a second seed value in a predetermined function, whereby secret sharing is implemented, and where the second seed value is permanently stored in said smart card, absent impermissible hindsight gleaned from Applicant's own disclosure.

Accordingly, Applicant respectfully submits the cited prior art fails to render Claim 1 unpatentable, at least by virtue that it fails to teach or suggest each of the recited limitations. Reconsideration and removal of this 35 USC 103(a) rejection is requested. Applicant also respectfully requests reconsideration and removal of the

rejections of Claims 2-4, at least by virtue of these claims' ultimate dependence from patentably distinct base Claim 1.

Regarding independent system claim 5, it similarly recites, in part, "access control processing means comprising means for generating said scrambling key by calculating the Y-intercept of a line on said Euclidean plane by said first seed value and a second seed value which is permanently stored in said smart card and means for descrambling." (emphasis added). Accordingly, Applicant respectfully submits the cited prior art also fails to render present Claim 5 unpatentable. Reconsideration and removal of this rejection is requested. Applicant also respectfully requests reconsideration and removal of the rejection of Claims 6-7, at least by virtue of these Claims' ultimate dependence from patentably distinct base Claim 5.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
A. Eskicioglu.

By: Paul P. Kiel
Attorney for Applicant
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: April 20, 2005